Arizona State Treasurer's Office
Request for a Merchant ID (MID) and
Payment Card Industry Data Security Standard (PCI-DSS) & Merchant Responsibilities Acknowledgement

In order for your agency to have the ability to accept and process credit cards, the Arizona State Treasurer Office (ASTO) administers the State of Arizona's Merchant process and contract so that you have the capability of accepting payment cards. The ASTO and Arizona Strategic Enterprise Technology Office (ASET) have contracted with merchant providers to supply the State agencies with Payment Card Industry Data Security Standard (PCI DSS) compliant options to accept payment cards online to sell goods and services to their customers. With these services, the State agencies' merchants must be in compliance with all rules, regulations and contractual provisions regarding the handling of payment cards. The regulations include the Payment Card Industry Standards and the Card Associations (MasterCard, VISA, American Express, Discover) merchant requirements.

All State agencies' merchants are required to comply with these regulations and requirements in order to continue to accept payment cards. In the event of non-compliance, the ASTO reserves the right to revoke those privileges until which time compliance is achieved.

Non-compliance with the Payment Card Industry standards puts the State of Arizona at risk for:

- Large monetary fines assessed to your agency and/or the State Arizona
- Loss of merchant status for your agency
- Possible loss of merchant status for all of State of Arizona
- Loss of faith, by the community in the State of Arizona's name

General Rules, Regulations, and Guidelines

A) Security

1. All State of Arizona Merchants are required to review the PCI DSS located online at https://www.pcisecuritystandards.org/.

2. If you process credit card data in any form (face-to-face or electronic), you need to be in compliance with PCI DSS.

3. All eCommerce gateways need to be PCI DSS certified and compliant with the State of Arizona's security requirements.

4. All electronically captured information must be in an encrypted secure socket layer (SSL) that meets the PCI DSS requirements with minimum need-to-know basis access to cardholder information.

5. Any vendor technical documents provided to the Merchant must be kept in a secure location and not shared with anyone else.

6. To meet the Arizona Revised Statute (A.R.S) 18-545 (Notification of Breach of Security System), the PCI-DSS payment card industry provisions and requirements, all suspected and/or confirmed security compromises need to be reported immediately to the ASTO and ASET. If a breach has occurred with the data you are storing, you are responsible for any and all externally imposed fines as well as the costs associated with bringing your location into compliance.

7. It is prohibited to store card information and card-validation codes (three-digit value printed on the signature panel of a card) on any State of Arizona computer, database or server. You must protect cardholder data by keeping it secure and confidential.

8. You must <u>not</u> collect card numbers and card information via e-mail, unsecured or network fax machines, or cell phones, as they are not secure formats.

9. You agree to maintain all card documentation containing card account numbers in a "secure" environment, restricting user access to payment card account numbers to a need-to-know basis. Secure environments include locked drawers, file cabinets in a locked office, and safes. Credit card receipts and card documentation needs to be treated in the same manner you would treat large sums of cash. Your agency is responsible for any losses due to inadequate internal controls. All card account numbers must be cross shredded within 24 hours of receipt and must comply with A.R.S. 44-7601.

10. You agree not to disclose or acquire any information concerning a cardholder's account without the cardholder's consent. You will not sell, purchase, provide, disclose or exchange card account information or any other transaction information.

11. Treat the following as high-risk transactions: use of anonymous e-mail address, shipping address from overseas, prisons, hospitals, or mail drops.

Name of State Agency: _____

Approval: _____
Agency Head Printed Name

Approval*: _____ _____
Agency Head Signature Date

* By signing this form your agency is approving the establishment of this merchant account and assumes responsibility for compliance with the Payment Card Industry Data Security Standards and the State of Arizona policy and guidelines as outlined above and in the attached document.

- Please call 602-542-7844 or email PCI@aztreasury.gov with questions.
- Please complete and return scanned copy to: Bankind@aztreasury.gov or
  State Treasurer's Office-Banking Division/PCI
  1700 W. Washington STE 102
  Phoenix, AZ 85007

Additional information on PCI DSS may be obtained by visiting the PCI Security Standards Council website at: https://www.pcisecuritystandards.org.